Table of Contents Author Index Home
Get Acrobat Reader Get Postscript Version Get PDF Version

The Saga of the One-Way Wire
or You Can't Get There From Here

Frank Lovato, NAVOCEANO MSRC
Mike Miller, Grumman Data Systems Corporation

Introduction

The One-Way Wire is what we call the connection between the unclassified and classified systems at the Naval Oceanographic Office (NAVOCEANO) Major Shared Resource Center (MSRC). In discussions with computer security people about the security aspects of creating a one-way wire, the immediate reaction was generally a loud and emphatic , "You can't do that!" Hence, the title of our discussion. Before discussing the technical aspects of connecting an unclassified computer system to a classified computer system in a secure environment, it is important to understand why we would attempt to do such an unprecedented thing.

Mission

The Naval Oceanographic Office (NAVOCEANO) is located at the Stennis Space Center in Mississippi and was originally established in 1830 as the Depot of Charts and Instruments. It is the largest subordinate command within Commander, Naval Meteorology and Oceanography Command and is responsible for providing oceanographic products and services to all elements of the Department of Defense (DoD). The NAVOCEANO mission is to "To acquire and analyze global ocean and littoral (off shore) data to provide specialized operationally significant products and services for war fighters, and civilian, national and international customers". This mission results in the collection of enormous amounts of data and requires world class supercomputer processing speeds and capabilities to process these data to meet the time critical user requirements..

Data Acquisition

Using ships, aircraft, satellites, and data buoys, NAVOCEANO collects and processes oceanographic, acoustic and mapping, charting, and geodesy data. Data are also obtained through international cooperative programs and data exchange agreements. These data are organized into databases and tactical oceanographic forecasts are produced using these data. These forecasts are then disseminated to ensure safe and accurate navigation, effective employment of sensor systems, and effective deployment of tactical and strategic weapons systems. NAVOCEANO provides forecast products and services for hydrography, mine warfare, shallow-water antisubmarine warfare, Arctic operations and special operations force. There is not a ship in the Navy that gets underway, an aircraft that flies, or a submarine under the ocean that does not depend on oceanographic forecast products from NAVOCEANO.

NAVOCEANO has technical control of seven multipurpose survey ships that conduct hydrographic, acoustic, oceanographic, and bathymetric data gathering surveys in littoral seas and oceans. Ships are now being deployed that have been designed from the keel up to perform acoustic, oceanographic, bathymetric, geomagnetic, gravity, and hydrographic data gathering survey operations, and are considered the ultimate answer to littoral or off-shore warfare support.

Specially equipped P-3 aircraft leased from the Naval Research Laboratory and operational fleet aircraft are used to collect bathythermographic, sea surface temperature, ambient noise, ice observation, and wave height data. These aircraft also take part in fleet exercises and, upon returning to the airfield, provide key information via a meteorology and oceanography theater center.

NAVOCEANO deployed over 200 drifting buoys last year from Air National Guard and Coast Guard aircraft to collect meteorological and oceanographic data. Hydrographic surveys are conducted worldwide to meet legal obligations to provide data necessary to ensure the safe navigation of American ships outside U.S. territorial waters. Requests for hydrographic products are submitted by approved DoD organizations to the Defense Mapping Agency (DMA), which tasks the Navy to survey in data-deficient areas. These data and data products are also collected to produce new or revised harbor, approach, coastal, and combat charts throughout the world.

Oceanographic Forecast Products

Sophisticated computer models have been developed to describe the physical characteristics of the ocean and its interaction with the atmosphere. Near real time projections are produced for DoD users around the world. NAVOCEANO support to undersea operations includes the collection and subsequent processing of data that results in oceanographic forecast products that ensure secure, covert, and precise navigation as well as detection of all submerged hazards to navigation within the submarine operating area. The products are generated for the assigned submarine operating areas that bound errors in navigation, fire-control, and missile guidance subsystems. NAVOCEANO provides tactical oceanographic publications with a wide range of environmental data presented in graph, chart, table, and text format to given users historical and climatologically predictive representations of data. Particular emphasis is placed upon providing capabilities the fleet and mobile teams with on-site environmental predictive systems to support real-time tactical decision systems.

The NAVOCEANO Warfighting Support Center

The Warfighting Support Center (WSC) was established within NAVOCEANO in 1993. Its mission is to qualitatively and quantitatively define the ocean environment for the Warfighter or other government agencies operating in the littoral region. Some products are intended for long-term planning purposes and so immediacy of delivery is not an issue. Other products are required within hours of the initial request and require a fast and dependable method of moving potentially large volumes of data. Still a third type of product is time-perishable because of its inherent description of dynamic ocean conditions. For example, a 3-D ocean analysis or wave forecast is only valid for a specific time period (analogous to a weather forecast). The product must reach the customer in time to put the information to use.

The WSC also provides infrared and visual imagery analyses of ocean thermal fronts and eddies and disseminates circulation model products, such as mine drift and oil spill drift, produced on the MSRC supercomputers. In support of Joint Littoral Warfare (JLW) and Special Operations Forces (SOF) , the WSC has implemented man-machine interactive high-resolution ocean models which can address the complexity of the littoral environment. Major capabilities were recently added for applying value-added information to all-source satellite imagery for tactical littoral SOF products within customer driven time frames. The WSC, using state-of-the-art technology, is an all-source data fusion center for the receipt and assimilation of satellite and in-situ oceanographic data.

The Major Shared Resource Center

NAVOCEANO administers and operates one of four DoD High Performance Computing (HPC) MSRCs established in October 1994 under the auspices of the DoD HPC modernization Program. The NAVOCEANO MSRC currently consists of an unclassified Cray C90, a classified Cray J-916se and a Y-MP2E file handler. Other systems operated within the MSRC include SGI Power Challenge Arrays (PCAs) for both classified and unclassified processing as well as SGI ONYX systems for classified and unclassified scientific data visualization. The NAVOCEANO MSRC is scheduled a major expansion in support of the DoD basic research, exploratory advanced development, and the operational efforts of the DoD science and technology (S&T) program.

Classified Supercomputer Support

Since the initial implementation of the NAVOCEANO Supercomputer Center, originally called the Primary

Oceanographic Prediction System (POPS), support has also been provided to classified users, first with a Cray X-MP and then later by a Cray Y-MP8. The classified system is operated in a closed classified network in a System High security environment.

Tape Transferral

The generation of some classified oceanographic forecast products often requires access to some data resident on the unclassified system. Some data are unsensitive and unclassified by their nature but require merging with other more sensitive data streams and processes to create classified products. Initially tapes were used to transfer the data. Certain users on the unclassified computer systems were allowed to write data to tape that the MSRC operations staff would manually move to the classified system for processing. Rigorous operating procedures were implemented to control the transferral and to limit who was allowed to request the manual tape transferrals.

The time required making this manual data transferral depended greatly upon the activity within the operations area. Initially, the manual response met the time frame necessary to produce the time sensitive oceanographic forecast products. As activity on the classified system increased, users of the classified system not directly involved with tactical fleet support began to use the tape facilities to transfer data from the unclassified system. Traffic began to increase and since tape drive availability was limited, longer and longer delays were encountered.

Enter the One-Way Wire

Realizing the manual tape operation was slow and cumbersome, on-site Grumman Data Systems and Cray analysts began a study to determine the feasibility of accessing unclassified data from the classified system in an automated and secure manner. With such a capability, very large data files, such as high-resolution satellite imagery, could be accessed from the classified computer systems for analysis, annotation and manipulation before being forwarded to the end-user. Quicker data movement from the unclassified system to the classified system would result in more rapid product turn-around. This capability would also permit implementation of automated data transferrals to support classified numerical model simulations and forecast products to be generated and provided to the customer every day, reliably and on time.

Since its initial implementation at NAVOCEANO, the Cray UNICOS Operating System had always been operated with the Multi Level Security (MLS) feature turned on. Since all users were configured at the same security level, the MLS code was continuously exercised but all access determination tests were null. To move these data from the unclassified to the classified system, the task was to use MLS to configure certain users and access ports to a security level different from the other users and then to determine if the data could be transferred while maintaining appropriate security. To avoid possible security conflicts during testing and development, the classified Cray Y-MP2E file handler and the classified Cray Y-MP8 were used as the test vehicle.

Technical Description

The first step in our quest to connect the classified to the unclassified system was to define what we were going to accomplish and how it was going to fit into out present environment. A chart was drawn up showing changes and interactions of file systems, users and networks between the proposed classified and unclassified systems. This chart was also used as the lead into the presentation required for implementation of the planned changes.

The next step was to confirm that MLS did work. A level 1 test was set up on the Y-MP8 system. A level 1 directory was defined and tests accounts were set to level 1. Analysis confirmed that a level 0 user could not access level 1 data.

The YMP-8 system was then set up as the server and the Y-MP2e became the client. This configuration was chosen because the Y-MP2e was the production server and in this way NFS could be selected up or down, file systems exported and what changes that could be introduced without interfering with production.

The network connection was defined next. The interface to the network was defined with the restrictions that access level was set to 1 and the connection was defined as point to point.

The spnet.conf, which defines the network security, was more of a challenge. In the nal (network access list), the minimum and maximum levels were set to 0 and 1 respectively, with no compartments. Ipso was defined as cipso and doi (domain of influence) was defined as 1.

A cipso map was defined with level1 = 1 with no compartments. This defines incoming data labels with a level of one are equal to the internal level of one. This map is tied to the doi through the doi tag. If the network which has a doi defined is going to the outside world, then the doi tag must be requested from the Internet Assigned Numbers Authority which will assign a unique number. Because our network was between two machines and nowhere else we could choose our own number.

A wal (workstation access list) was defined to further restrict access to the link. The first definition was *.* = none. This restricts all access by any person or program to the network. Next nfs access for a specific account was enabled. This took the form act1, act2, act3, ect, = nfs. The placement of these commands within the nal list are hierarchical.

Therefore, all access was denied, then only the desired access was enabled. Reversing the commands would have not access because the last command would have denied access to the network.

The uid mapping defined only those accounts that were to have access to the nfs defined connection. This mapping must be in place for any joint nfs/MLS implementation. This was a useful restriction as an undefined account was denied access to nfs on the client.

The last variable on the server was to define the entry in the export file of the directory to be exported via nfs. This was setup as a read only entry and restricted users from writing data into the directory from the client system.

The client machine was set up in the same manner. The difference being the cipso map, which mapped incoming labels at level 1 to local level of 0 and the interfaces file that set the network interface level to 0 only.

The nfs directory was next mounted. The directory was exported and appeared in the list when the exportfs command was issued at the server. The mount command was issued at the client machine and an error message appeared "Server not responding". This was the expected result.

The mount would retry while running in background until it would time out. We had expected the request to leave the client at level 1 and return at the same level. Mountd would attempt to return the request at the level of the directory to a level 1. This meant that in order to use the directory
the users would have to be able to raise their level to a 1. This could lead to an inadvertent access to the one-way network. One of the intended advantages was that no user was to have a level 1 access to the network.

The Cray site analyst, Orvin Tobiason, contacted Technical Support in Eagan, who came to the rescue. After reviewing the code and several network traces, several code changes were recommended.

The first change was to mountd. Here the code was changed to use the subject level of the request, rather than the object level of the directory. All traffic coming from the client was assured to be level 1 with the use of cipso mapping 1 = 1. To keep the return level at 1 nfs kernel code was changed. The line that moved the subject level to the current working level was deleted. This meant the incoming request level that was 1 was retained and also became the outgoing level. This change was in the nfs section of the kernel therefore, nfs was the only protocol to return the correct label over the interface. The server now returned the data to the client at level 1.

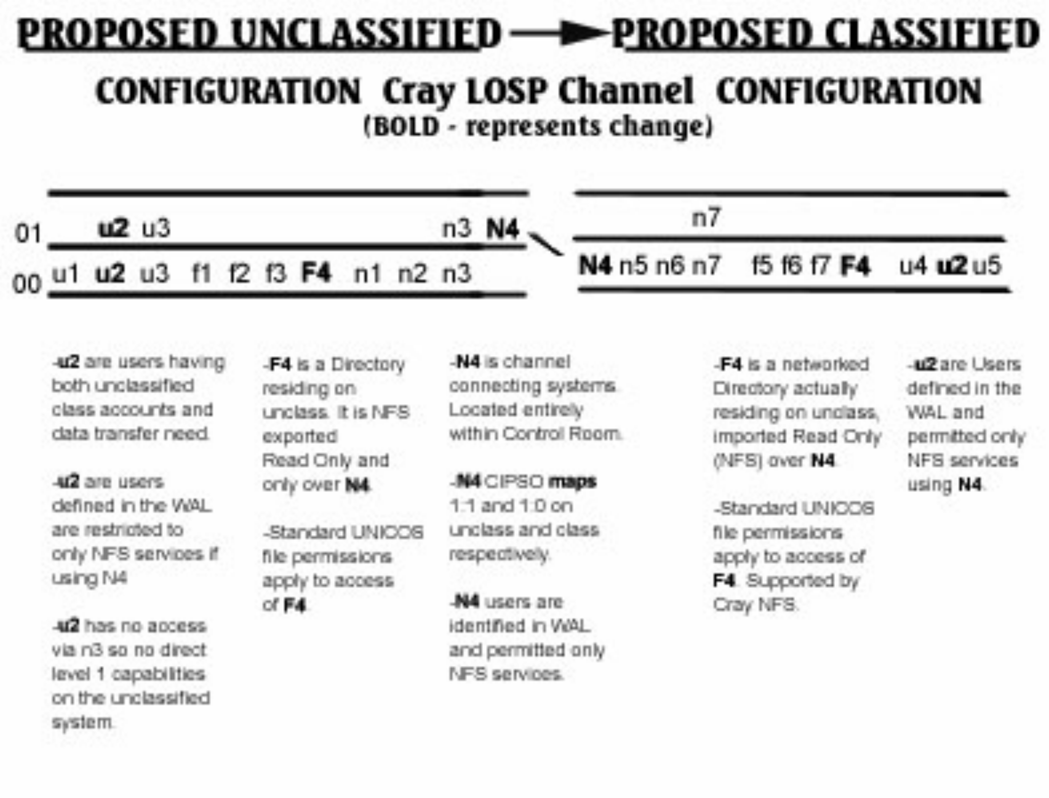
This allowed the data out of the server interface that was cipso mapped to level 1 and in the client interface that was also mapped to level 1. The incoming level was then remapped to level 0. The cipso map on the client being 0 = 1. The data was now on the client at a level usable to anyone who was defined in the wal.

The non wall defined user was not aware that level one data was present on the host system. When an undefined user attempted an ls command on the NFS mounted directory, the prompt returned without comment. In this manner the undefined user was unaware of the NFS mounted directory. If the undefined user attempted to cd to the NFS mounted directory, the prompt returned without comment. Once again this user was unaware of a security violation. The security log was dumped and the violations were verified.

The users and all of the file systems remained defined at level zero. There was no change for the users and down time was kept to just a reboot. The network was protected on both the server and client sides at level 1. No network traffic other than the "fixed" NFS could traverse the network.

Conclusion

The "One-Way Wire" implementation has proven to be quite successful in meeting the timeliness requirements for creating and disseminating oceanographic forecast products to the fleet while maintaining the necessary security protection. Since the UNIX operational scripts were developed and checked out, the data transferal operation has become transparent in its ease of use. In addition to the WSC, others using the classified system have gained access to data previously unavailable. The system has been accredited by the NAVOCEANO Commanding Officer who is the Designated Approval Authority (DAA) and was recently surveyed by the Defense Information Security Agency (DISA) for certification.



PROPOSED UNCLASSIFIED → PROPOSED CLASSIFIED

CONFIGURATION Cray LOSP Channel CONFIGURATION

(BOLD - represents change)

01
u2 u3
n3 **N4**
00
u1 **u2** u3 f1 f2 f3 **F4** n1 n2 n3
n7
N4 n5 n6 n7 f5 f6 f7 **F4** u4 **u2** u5

-**u2** are users having both unclassified class accounts and data transfer need.

-**u2** are users defined in the WAL are restricted to only NFS services if using N4

-**u2** has no access via n3 so no direct level 1 capabilities on the unclassified system.

-**F4** is a Directory residing on unclass. It is NFS exported Read Only and only over **N4**.

-Standard UNICOS file permissions apply to access of **F4**.

-**N4** is channel connecting systems. Located entirely within Control Room.

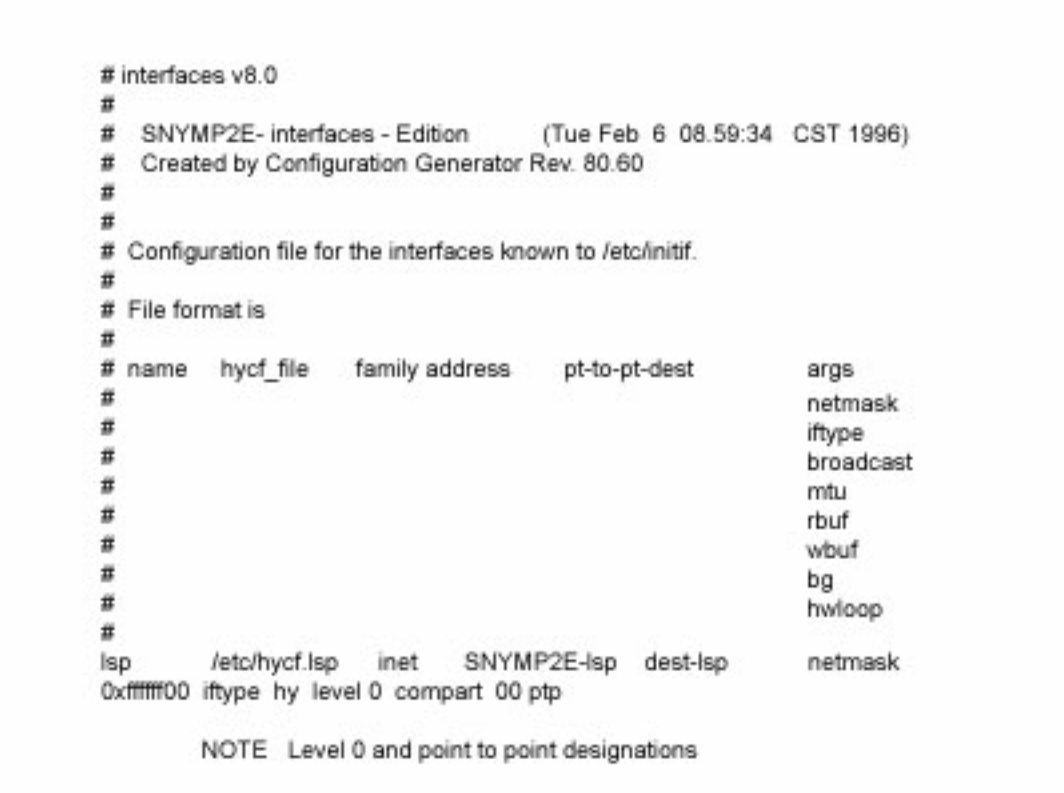
-**N4** CIPSO **maps** 1:1 and 1:0 on unclass and class respectively.

-**N4** users are identified in WAL and permitted only NFS services.

-**F4** is a networked Directory actually residing on unclass, imported Read Only (NFS) over **N4**.

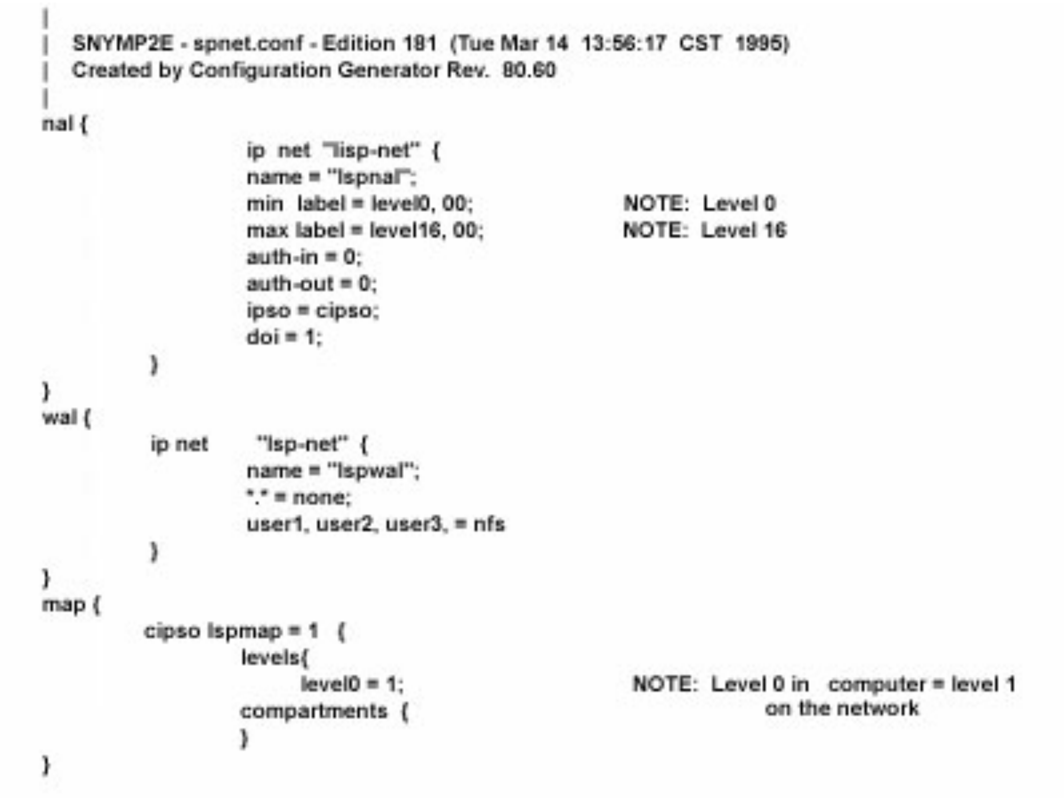
-Standard UNICOS file permissions apply to access of **F4**. Supported by Cray NFS.

-**u2** are Users defined in the WAL and permitted only NFS services using **N4**.

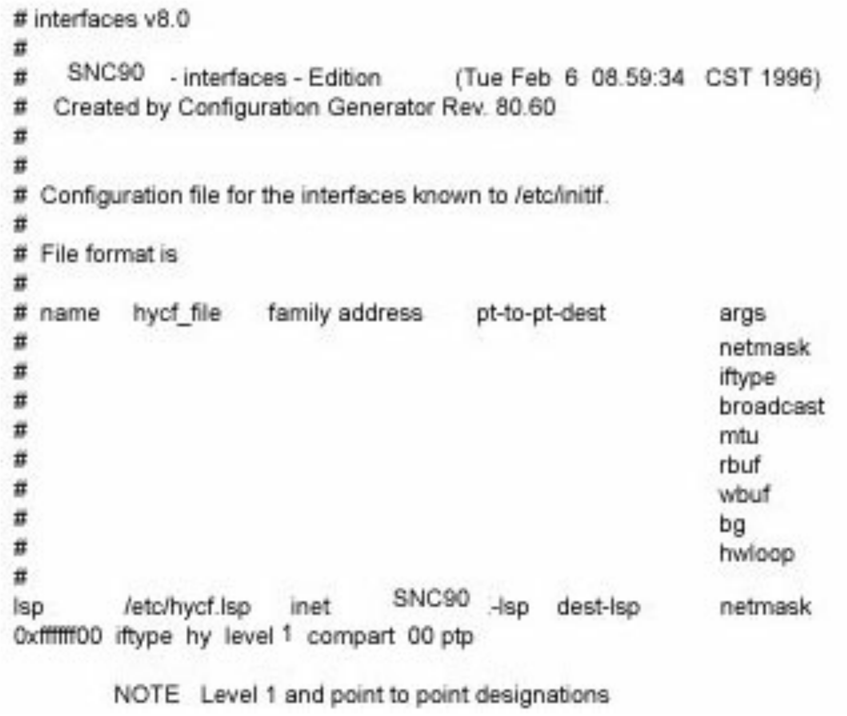


```
# interfaces v8.0
#
#   SNYMP2E- interfaces - Edition        (Tue Feb  6  08.59:34   CST 1996)
#   Created by Configuration Generator Rev. 80.60
#
#
# Configuration file for the interfaces known to /etc/initif.
#
# File format is
#
# name    hycf_file     family address      pt-to-pt-dest            args
#                                                                    netmask
#                                                                    iftype
#                                                                    broadcast
#                                                                    mtu
#                                                                    rbuf
#                                                                    wbuf
#                                                                    bg
#                                                                    hwloop
#
lsp          /etc/hycf.lsp     inet     SNYMP2E-lsp    dest-lsp        netmask
0xffffff00  iftype  hy  level 0  compart  00 ptp

           NOTE   Level 0 and point to point designations
```

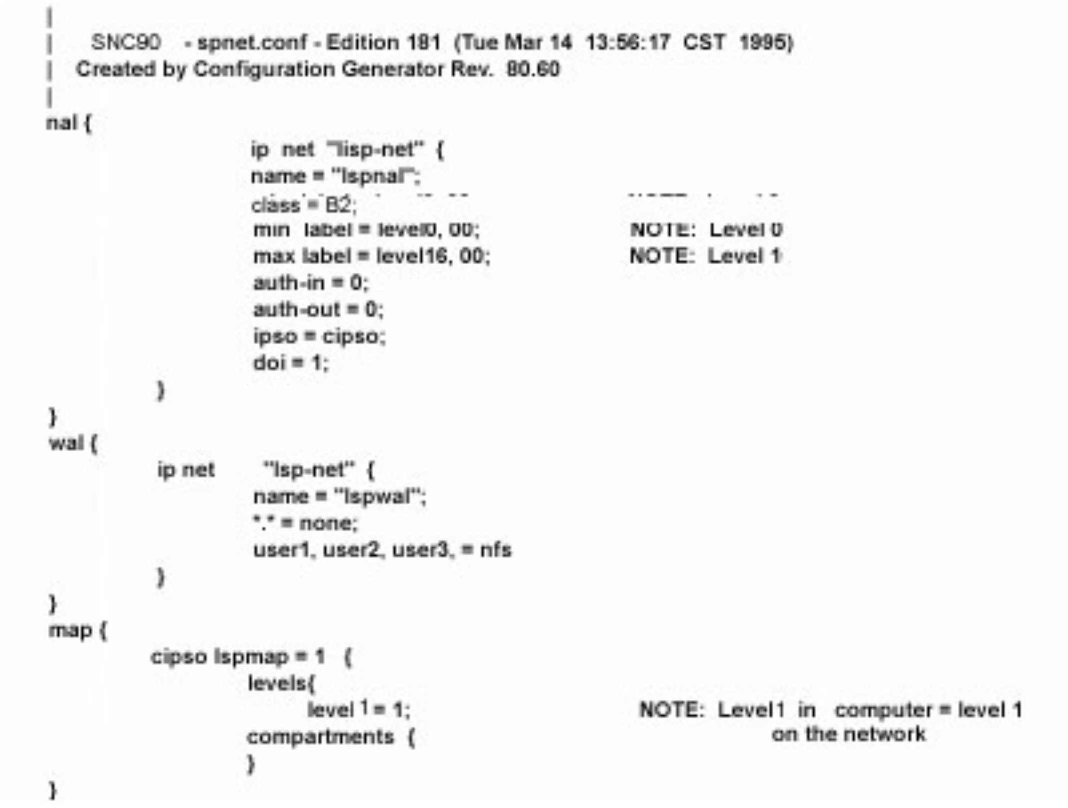


```
|
|   SNYMP2E - spnet.conf - Edition 181  (Tue Mar 14  13:56:17  CST  1995)
|   Created by Configuration Generator Rev.  80.60
|
nal {
                    ip  net  "lisp-net"  {
                    name = "lspnal";
                    min  label = level0, 00;                NOTE:  Level 0
                    max label = level16, 00;                NOTE:  Level 16
                    auth-in = 0;
                    auth-out = 0;
                    ipso = cipso;
                    doi = 1;
          }
}
wal {
          ip net       "lsp-net"  {
                    name = "lspwal";
                    *.* = none;
                    user1, user2, user3, = nfs
          }
}
map {
         cipso lspmap = 1   {
                   levels{
                         level0 = 1;                        NOTE:  Level 0 in   computer = level 1
                   compartments  {                                       on the network
                   }
}
```

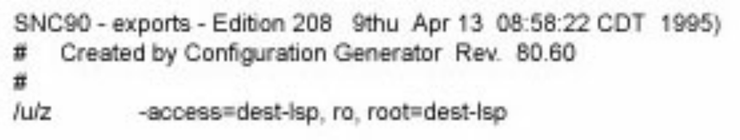


```
# interfaces v8.0
#
#    SNC90  - interfaces - Edition        (Tue Feb 6  08.59:34  CST 1996)
#   Created by Configuration Generator Rev. 80.60
#
#
#  Configuration file for the interfaces known to /etc/initif.
#
#  File format is
#
#  name    hycf_file     family address      pt-to-pt-dest           args
#                                                                    netmask
#                                                                    iftype
#                                                                    broadcast
#                                                                    mtu
#                                                                    rbuf
#                                                                    wbuf
#                                                                    bg
#                                                                    hwloop
#
lsp        /etc/hycf.lsp    inet      SNC90 -lsp   dest-lsp          netmask
0xffffff00  iftype  hy  level 1  compart  00 ptp
```

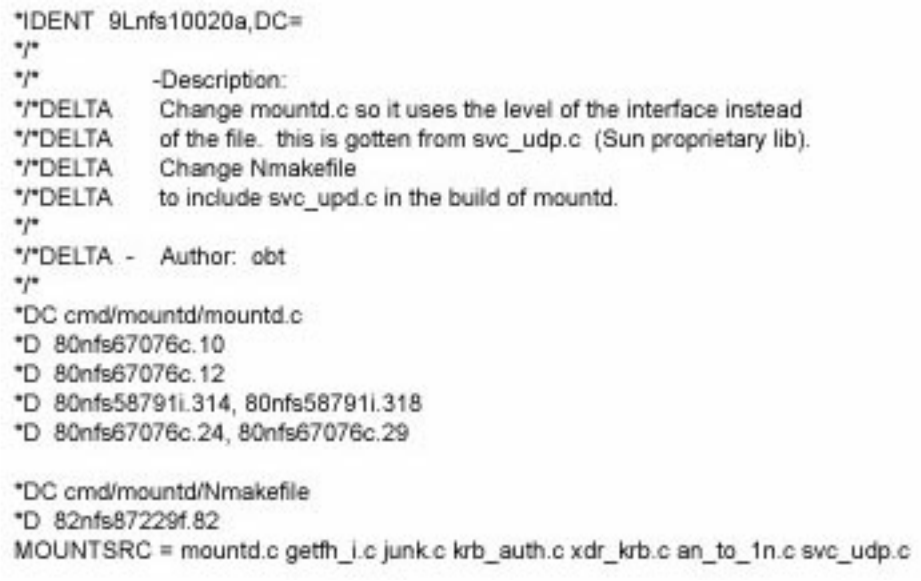
NOTE   Level 1 and point to point designations



```
|
|    SNC90   - spnet.conf - Edition 181  (Tue Mar 14  13:56:17  CST  1995)
|   Created by Configuration Generator Rev.  80.60
|
nal {
                    ip  net  "lisp-net"  {
                    name = "lspnal";
                    class = B2;
                    min  label = level0, 00;            NOTE:  Level 0
                    max label = level16, 00;            NOTE:  Level 1
                    auth-in = 0;
                    auth-out = 0;
                    ipso = cipso;
                    doi = 1;
            }
}
wal {
            ip net       "lsp-net"  {
                    name = "lspwal";
                    *.* = none;
                    user1, user2, user3, = nfs
            }
}
map {
           cipso lspmap = 1   {
                    levels{
                          level 1 = 1;                   NOTE:  Level1  in   computer = level 1
                    compartments  {                                      on the network
                    }
}
```

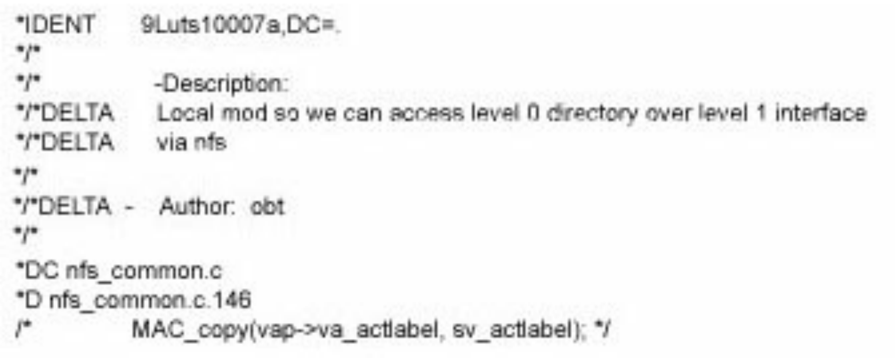


```
SNC90 - exports - Edition 208   9thu  Apr 13  08:58:22 CDT  1995)
#    Created by Configution Generator  Rev.  80.60
#
/u/z          -access=dest-lsp, ro, root=dest-lsp
```



```
*IDENT  9Lnfs10020a,DC=
*/*
*/*              -Description:
*/*DELTA      Change mountd.c so it uses the level of the interface instead
*/*DELTA      of the file.  this is gotten from svc_udp.c  (Sun proprietary lib).
*/*DELTA      Change Nmakefile
*/*DELTA      to include svc_upd.c in the build of mountd.
*/*
*/*DELTA -    Author:  obt
*/*
*DC cmd/mountd/mountd.c
*D  80nfs67076c.10
*D  80nfs67076c.12
*D  80nfs58791i.314, 80nfs58791i.318
*D  80nfs67076c.24, 80nfs67076c.29

*DC cmd/mountd/Nmakefile
*D  82nfs87229f.82
MOUNTSRC = mountd.c getfh_i.c junk.c krb_auth.c xdr_krb.c an_to_1n.c svc_udp.c
```



```
*IDENT      9Luts10007a,DC=.
*/*
*/*              -Description:
*/*DELTA      Local mod so we can access level 0 directory over level 1 interface
*/*DELTA      via nfs
*/*
*/*DELTA -    Author:  obt
*/*
*DC nfs_common.c
*D nfs_common.c.146
/*             MAC_copy(vap->va_actlabel, sv_actlabel); */
```

Acknowledgment

The authors would like to recognize Orvin Tobiason of Cray Research and Jesse Pollard of Northrop Gruman Data Systems for their hard work in helping create the "One-Way Wire". We also wish to thank LCDR Charles D. (Bud) Dailey and Joseph Stinus of the NAVOCEANO Warfighting Support Center for their assistance in preparing this paper.

Table of Contents | Author Index | CUG Home Page | Home